CLAIMS

I claim:

1. A method for on-line mass distribution of data products to end users, the method comprising:

maintaining a first portion of each of said data products at a first location;

maintaining a second portion of each of said data products at a second location;

for each of said end users, confirming the end user's entitlement to one of said data products;

obtaining a first portion of said one of said data products from said first location and a second portion of said one of said data products from said second location;

combining said first portion of said one of said data products and said second portion of said one of said data products; and

providing said combined first portion and second portion to said user.

2. The method of claim 1, wherein said data products include geographic databases.

3. The method of claim 1, wherein said data products include digital copies of movies.

4. The method of claim 1, wherein said data products include digital copies of musical songs.

5. The method of claim 1, further comprising the step of:

encrypting said first portion of each of said data products.

6. The method of claim 1, further comprising the step of:

prior to the step of combining, encrypting said first portion of one of said data products.

7. The method of claim 1, wherein said step of combining is performed at said second location.

8. A system for secure on-line mass distribution of data products to end users comprising:

an authorization server having associated therewith copies of first portions of a plurality of data products;

a plurality of data distribution terminals, each of which has associated therewith copies of second portions of said plurality of data products;

a communications system that provides for exchange of data between said authorization server and said plurality of data distribution terminals, and

a data distribution program that provides copies of said data products to those end users who are entitled to have said copies thereof, wherein said data distribution program provides a copy of a data product by combining a copy of the first portion of said data product obtained from said authorization server with a copy of the second portion of said data product obtained from one of said plurality of data distribution terminals.

9. The system of claim 8, wherein said authorization server also has associated therewith an authorization database containing data indicating entitlement by said end users to copies of said data products.

10. A system for securely conveying a data product, the data product defining a first portion and a second portion, the first portion defining at least one key to the second portion, the system comprising, in combination:

a first entity maintaining the first portion;

a second entity maintaining the second portion;

a first set of logic executable by the first entity to encrypt the first portion so as to produce an encrypted first portion that can be decrypted using a first decryption key, wherein the first entity sends the encrypted first portion via a telecommunications link to the second entity; and

a second set of logic executable by the second entity, upon receipt of the encrypted first portion, to record onto a storage medium the encrypted first portion and the second portion,

wherein the storage medium may be provided to a third entity, which, if provided with access to the first decryption key, can in turn access the data product.

11. The system of claim 10, wherein the first entity sends to the second entity, together with the encrypted first portion, an encrypted authorization key that can be decrypted using a second decryption key so as to reveal verification information indicative of an entity authorized to access the data product, and wherein the second set of logic is further executable to record onto the storage medium the encrypted authorization key.

12. The system of claim 11, wherein the second decryption key is derived as a function of an environmental parameter.

13. The system of claim 12, wherein the environmental parameter comprises an identification code associated with the entity authorized to access the data product.

14. The system of claim 11, wherein the third entity has access to the second decryption key, the system further comprising:

a third set of logic executable by the third entity to decrypt the encrypted authorization key, to thereby gain access to the verification information, and to use the verification information to validate use of the data product.

15. The system of claim 11, wherein the third entity has access to the second decryption key, the system further comprising:

a third set of logic executable by the third entity to decrypt the encrypted authorization information, to thereby gain access to the verification information, and to compare at least a portion of the verification information to predetermined information associated with the third entity so as to determine whether the third entity is authorized to access the data product.

16. The system of claim 15, wherein the predetermined information associated with the third entity comprises an identification code.

17. The system of claim 10, wherein the first entity sends to the second entity, together with the encrypted first portion, an encrypted authorization key that can be decrypted using a second decryption key so as to reveal verification information indicative of an entity authorized to store the data product.

18. The system of claim 17, wherein the second decryption key is derived as a function of an environmental parameter.

19. The system of claim 18, wherein the environmental parameter comprises an identification code associated with the entity authorized to store the data product.

20. The system of claim 17, wherein the third entity has access to the second decryption key, the system further comprising:

a third set of logic executable by the third entity to decrypt the encrypted authorization key, to thereby gain access to the verification information, and to use the verification information to validate storage of the data product.

21. The system of claim 17, wherein the third entity has access to the second decryption key, the system further comprising:

a third set of logic executable by the third entity to decrypt the encrypted authorization information, to thereby gain access to the verification information, and to compare at least a portion of the verification information to predetermined information associated with the storage medium so as to determine whether the storage medium is authorized to store the data product.

22. The system of claim 21, wherein the predetermined information associated with the storage medium comprises an identification code.

23. The system of claim 10, wherein the data product comprises geographic information and the third entity comprises a navigation system.

24. A method for securely conveying a data product, the data product defining a first portion and a second portion, the first portion defining at least one key to the second portion, the method comprising, in combination:

at a first entity, encrypting the first portion of the data product so as to produce an encrypted first portion that can be decrypted using a first decryption key;

sending the encrypted first portion via a telecommunications link from the first entity to a second entity;

receiving the encrypted first portion at the second entity;

at the second entity, recording onto a storage medium the encrypted first portion and the second portion; and

thereafter providing the storage medium to a third entity,

whereby, if the third entity has access to the first decryption key, the third entity may decrypt the encrypted first portion and thereby gain access to the data product.

25. The method of claim 24, further comprising sending to the second entity, together with the encrypted first portion, an encrypted authorization key that can be decrypted using a

second decryption key so as to reveal verification information indicative of an entity authorized to access the data product.

26. The method of claim 25, further comprising generating the second decryption key as a function of an environmental parameter.

27. The method of claim 26, wherein the environmental parameter comprises an identification code associated with the entity authorized to access the data product.

28. The method of claim 27, further comprising:

the third entity generating the second decryption key as the function of the identification code;

the third entity using the second decryption key to decrypt the encrypted authorization key and to thereby gain access to the verification information; and

the third entity using the verification information to validate storage of the data product.

29. The method of claim 25, further comprising:

the third entity using the second decryption key to decrypt the encrypted authorization key and to thereby gain access to the verification information; and

the third entity using the verification information to validate use of the data product.

30. The method of claim 29, wherein using the verification information to validate use of the data product comprises comparing at least a portion of the verification information to predetermined information associated with the third entity so as to determine whether the third entity is authorized to access the data product.

31. The method of claim 30, wherein the predetermined information associated with the third entity comprises an identification code.

32. The method of claim 24, further comprising sending to the second entity, together with the encrypted first portion, an encrypted authorization key that can be decrypted using a second decryption key so as to reveal verification information indicative of an entity authorized to store the data product.

33. The method of claim 32, further comprising generating the second decryption key as a function of an environmental parameter.

34. The method of claim 33, wherein the environmental parameter comprises an identification code associated with the entity authorized to store the data product.

35. The method of claim 34, further comprising:

the third entity generating the second decryption key as the function of the identification code;

the third entity using the second decryption key to decrypt the encrypted authorization key and to thereby gain access to the verification information; and

the third entity using the verification information to validate storage of the data product.

36. The method of claim 32, further comprising:

the third entity using the second decryption key to decrypt the encrypted authorization key and to thereby gain access to the verification information; and

the third entity using the verification information to validate storage of the data product.

37. The method of claim 36, wherein using the verification information to validate storage of the data product comprises comparing at least a portion of the verification information to predetermined information associated with the storage medium so as to determine whether the storage medium is authorized to store the data product.

38. The method of claim 37, wherein the predetermined information associated with the storage medium comprises an identification code.

39. The method of claim 24, wherein the data product comprises geographic information and the third entity comprises a navigation system.